NSC shall provide overall policy direction for the Information Security Program.

(b) *Administrator of General Services.* The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established under E.O. 12356. In accordance with E.O. 12356, the Administrator delegates the implementation and monitorship functions of the Program to the Director of the ISOO.

(c) *Information Security Oversight Office*—(1) *Composition.* The ISOO has a full-time director appointed by the Administrator of General Services with approval of the President. The Director has the authority to appoint a staff for the office.

(2) *Functions.* The Director of the ISOO is charged with the following principal functions that pertain to the Department of Defense:

(i) Oversee DoD actions to ensure compliance with E.O. 12356 implementing directives, for example, the ISOO Directive No. 1 and this part;

(ii) Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the Information Security Program;

(iii) Report annually to the President through the NSC on the implementation of E.O. 12356;

(iv) Review this Regulation and DoD guidelines for systematic declassification review; and

(v) Conduct on-site reviews of the Information Security Program of each DoD Component that generates or handles classified information.

(3) *Information Requests.* The Director of the ISOO is authorized to request information or material concerning the Department of Defense, as needed by the ISOO in carrying out its functions.

(4) *Coordination.* Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the ISOO are brought to the attention of the Director of Security Plans and Programs, ODUSD(P).

§159a.92 Department of Defense.

(a) *Management Responsibility.* (1) The DUSD(P) is the Senior DoD Information Security Authority having DoD-wide authority and responsibility to ensure effective and uniform compliance with and implementation of E.O. 12356 and its implementing ISOO Directive No. 1. As such, the DUSD(P) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The DUSD(P) or his designee may approve waivers or exceptions to the provisions of this part to the extent such action is consistent with E.O. 12356 and ISOO Directive No. 1.

(2) The heads of DoD Components may approve waivers to the provisions of this part only as specifically provided for herein.

(3) The Director, NSA/Chief, Central Security Service, under 32 CFR part 159, is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. In this regard, the Director, NSA, may approve waivers or exceptions to these special requirements. Except as provided in §159a.6 the authority to lower any COMSEC security standards rests with the Secretary of Defense. Requests for approval of such waivers or exceptions to established COMSEC security standards which, if adopted, will have the effect of lowering such standards, shall be submitted to the DUSD(P) for approval by the Secretary of Defense.

§159a.93 DoD components.

(a) *General.* The head of each DoD Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this part throughout the Component.

(b) *Military Departments.* In accordance with 32 CFR part 159 the Secretary of each Military Department shall designate a Senior Information Security Authority who shall be responsible for complying with and implementing this part within the Department.

(c) *Other Components.* In accordance with 32 CFR part 159, the head of each other DoD Component shall designate a Senior Information Security Authority who shall be responsible for complying

with and implementing this Regulation within their respective Component.

(d) *Program Monitorship.* The Senior Information Security Authorities designated under paragraphs (b) and (c) of this section, are responsible within their respective jurisdictions for monitoring, inspecting with or without prior announcement, and reporting on the status of administration of the DoD Information Security Program at all levels of activity under their cognizance.

(e) *Field Program Management.* (1) Throughout the Department of Defense, the head of each activity shall appoint, in writing, an official to serve as security manager for the activity. This official shall be responsible for the administration of an effective Information Security Program in that activity with particular emphasis on security education and training, assignment of proper classifications, downgrading and declassification, safeguarding, and monitorship, to include sampling classified documents for the purpose of assuring compliance with this part.

(2) Activity heads shall ensure that officials appointed as security managers either possess, or obtain within a reasonable time after appointment, knowledge of and training in the Information Security Program commensurate with the needs of their positions. The Director of Security Plans and Programs, ODUSD(P) shall, with the assistance of the Director, Defense Security Institute, develop minimum standards for training of activity security managers. Such training should result in appropriate certifications to be recorded in the personnel files of the individuals involved.

(3) Activity heads shall ensure that officials appointed as security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They also shall provide sufficient resources of time, staff, and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of the Information Security Program at all levels of the activity.

§ 159a.94 Information requirements.

(a) *Information Requirements.* DoD Components shall submit on a fiscal year basis a consolidated report concerning the Information Security Program of the Component on SF 311, ''Agency Information Security Program Data,'' to reach the ODUSD(P) by October 20 of each year. SF 311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the ODUSD(P). The ODUSD(P) shall submit the DoD report (SF 311) to the ISOO by October 31 of each year. Interagency Report Control Number 0230–GSA–AN applies to this information collection system as well as to that contained in § 159a.12.

§ 159a.95 Defense Information Security Committee.

(a) *Purpose.* The Defense Information Security Committee (DISC) is established to advise and assist the DUSD(P) and the Director, Security Plans and Programs (ODUSD(P) in the formulation of DoD Information Security Program policy and procedures.

(b) *Direction and Membership.* The DISC shall meet at the call of the DUSD(P) or the Director, Security Plans and Programs. It is comprised of the DUSD(P) as Chairman; the Director, Security Plans and Programs, as Vice Chairman; and the senior officials (designated in accordance with section E.3.a., DoD Directive 5200.1,[39] or their representatives) responsible for directing and administering the Information Security Program of the OJCS, the Departments of the Army, Navy, and Air Force, the Defense Intelligence Agency, the Defense Nuclear Agency, the National Security Agency, and the Defense Investigative Service. Other DoD Components may be invited to attend meetings of particular interest to them.

[39] See footnote 1 to § 159a.3